Facility Access Control Hacking

Intelligence Dissemination Report

Regional Operations and Intelligence Center (ROIC) Infrastructure Protection Unit ~ ROIC202401-01525X

18 January 2024

Event Details:

Recently, a NJ high school student utilized a "Flipper Zero" tool to gain access to interior and exterior school doors. An attentive school administrator conducted an audit and identified the suspicious activity. The student admitted to obtaining a teacher's ID card, copying the Radio Frequency Identification (RFID) with the "Flipper Zero", and distributing additional access cards to other students.

Key Findings:

"Flipper Zero" devices can be purchased online and have the capability to read RFID frequencies and copy them to a key tag/fob/card, etc. It is unknown if the devices can be used for EZ Pass tags or vehicle keys, but they are marketed to have the ability to hack radio protocols, access control systems, hardware, and more. Threat actors have utilized social media platforms to propagate this tool to attempt access to sensitive areas across certain domains, including the energy sector.

Options for Consideration:

- **RFID Hardening:** Individuals and organizations concerned about RFID/NFC cloning can defeat this attack vector by employing blocking wallets or sleeves which prevent the device from reading access cards. **The most effective defense method is preventing initial access to the card.** It can take up to 30 seconds for each scan, during which the device needs to remain in very close proximity (typically within 1-4 inches) to the card.
- **Access Control Enhancement:** Utilize a system which also includes a PIN in addition to scanning the badge. If someone was able to duplicate the badge, they would still need the appropriate PIN to enter. Using a system that requires a badge scan to exit can prevent duplicate badge numbers from entering the building.
- **Audits:** Scheduled audits and system testing should be part of a facility's security plan. Report suspicious activity to local law enforcement immediately.

Additional Resources: https://www.cyber.nj.gov/alerts-advisories/flipper-zero
Sources: Intelligence Community Reporting, Open Source Reporting, Law Enforcement
Source Reliability: Reliable
Dissemination: Law Enforcement, NJ Schools, Infrastructure Partners

Contact Information: *Any questions about this product should be directed to the Office of the ROIC Infrastructure Protection Unit (609) 963-6900, or NJROICIPU@njsp.gov.*
Suspicious Activity Reporting: *Suspicious activity with a possible nexus to terrorism should be reported to NJOHSP CT Watch at 866.4SAFENJ (866.472.3365) or tips@njohsp.gov.*